aws competency

AWS Security Competency

Technology Partner Validation Checklist

April 2019
Version 3.0

aws partner network

Table of Contents

Introduction

The goal of the AWS Competency Program is to recognize AWS Partner Network Partners ("APN Partners") who demonstrate technical proficiency and proven customer success in specialized solution areas. The Technology Partner Validation Checklist ("Checklist") is intended for APN Partners who are interested in applying for AWS Competency. This Checklist provides the criteria necessary to achieve the AWS Security Competency designation under the AWS Competency Program. APN Partners undergo an audit of their capabilities upon applying for the specific Competency. AWS leverages in-house expertise and may also utilize a third-party firm to facilitate the audit. AWS reserves the right to make changes to this document at any time in its sole discretion.

Expectations of Parties

It is expected that APN Partners will review this document in detail before submitting an application for the AWS Competency Program, even if all of the prerequisites are met. If items in this document are unclear and require further explanation, please contact your AWS Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Program Office if further assistance is required.

When ready to submit a program application, APN Partners should complete the Partner Self-Assessment column of the AWS Competency Program Validation Checklist set forth below in this document.

To submit your application:

1. Log in to the APN Partner Central (https://partnercentral.awspartner.com/), as Alliance Lead
2. Select "View My APN Account" from the left side of the page
3. Scroll to "Program Details" section
4. Select "Update" next to AWS Competency you wish to apply for
5. Fill out Program Application and Click "Submit"
6. Email completed Self-Assessment to competency-checklist@amazon.com

If you have any questions regarding the above instructions, please contact your PDR/PDM.

AWS will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your audit or to request additional information.

APN Partners should prepare for the audit by reading the Checklist, completing a self-assessment using the Checklist, and gathering and organizing objective evidence to share with the auditor on the day of the audit.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the audit. The best practice is for the APN Partner to make the following personnel available for the audit: one or more highly technical AWS certified engineers/architects, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation. APN Partners should ensure that they have the necessary consents to share with the auditor (whether AWS or a third-party) all information contained within the objective evidence or any demonstrations prior to scheduling the audit.

AWS Security Competency Program Prerequisites

The following items will be validated by the AWS Competency Program Manager. AWS may also utilize a third-party firm to facilitate this audit. Missing or incomplete information must be addressed prior to scheduling of the audit ("Technology Validation Review").

1.0 APN Program Membership		Met Y/N
1.1 Program Guidelines	The APN Partner must read the Program Guidelines and Definitions before applying to the DevOps Competency Program. Click here for Program details	
1.1 Technology APN Partner Tier	APN Partner must be an Advanced Tier APN Technology Partner before applying to the Security Competency Program.	
1.2 Solution Category	APN Partner to identify the Segment Category for their solution: ☐ **Network and Infrastructure Security** ☐ **Host and Endpoint Security** ☐ **Data Protection and Encryption** ☐ **Governance, Risk, and Compliance** ☐ **Logging, Monitoring, Threat Detection, and Analytics** ☐ **Identity and Access Control** ☐ **Vulnerability and Configuration Assessment** ☐ **Application Security** Deployment Model: ☐ **SaaS on AWS** ☐ **SaaS outside AWS** ☐ **BYOL on AWS** ☐ **BYOL On-premises**	

2.0 Case Studies		Met Y/N
2.1 Security - Specific Case Studies	APN Partner must have four (4) unique customer Case Studies specific to a Security solution under review. It is acceptable for an APN Partner solution to be comprised of multiple products to address a category use case. Each of the four (4) Case Studies must relate to an example of the APN Partner Solution being used in one of the six Segment Categories: For each Case Study, the APN Partner must provide the following information: ▪ Name of the customer ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ Third party applications or solutions used ▪ Date the reference entered production ▪ Outcome(s)/results This information will be requested as part of the program application process in APN Partner Central. The information provided as part of this Case Study can be private and will not be made public. All four (4 of the Case Studies provided will be examined in the Documentation Review of the Technical Validation. The Case Study will be removed from consideration for inclusion in the Competency if the APN Partner cannot provide the documentation necessary to assess the Case Study against each checklist item, or if there were any of the checklist items are not met.	

	Case Studies must describe deployments that have been performed within the past 18 months, and must be for projects that are in production with customers, rather than in a 'pilot' or proof of concept stage.	
2.2 Publicly Available Case Studies	Publicly available case studies are used by AWS upon approval into the Competency to showcase the APN Partner's demonstrated success based on measurable KPIs with the solution and provide customers with confidence that the APN Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives. Two (2) of the four (4) customer deployments associated with the Case Studies must be publicized by the APN Partner as publicly available case studies. These publicly available case studies may in the form of formal case studies, white papers, videos, or blog posts.	
	Publicly available case studies must be easily discoverable from the APN Partner's website, e.g. it must be possible to navigate to the publicly available case study from the APN Partner's home page, and the APN Partner must provide links to these publicly available case studies in their application.	
	Publicly available case studies must include the following: ▪ References to the customer name, APN Partner name, and AWS ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ How AWS services were used as part of the solution ▪ Outcome(s)/results	
3.0 AWS Security Web Presence and Thought Leadership		**Met Y/N**
3.1 APN Partner AWS Landing Page	An APN Partner's internet presence specific to their AWS Security Solutions provides customers with confidence about the APN Partner's capabilities and experience. APN Partner must have an AWS Landing Page that describes their AWS Security solution, links to their publicly available case studies, lists technology partnerships, and provides any other relevant information supporting the APN Partner's expertise related to Security Competency and highlighting the partnership with AWS. This AWS-specific Security page must be accessible from the APN Partner's home page. The home page itself is not acceptable as an AWS Landing Page unless APN Partner is a dedicated Security company and home page reflects APN Partner's focus on Security Competency.	
3.2 Security Thought Leadership	AWS Security Competency Partners are viewed as having deep domain expertise in Security Competency having developed innovative solutions that leverage or help manage AWS services. APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner's focus on and expertise in Security links must be provided to examples of materials published within the last 12 months.	
4.0 Business Requirements		
4.1 Field-Ready Toolkits	APN Partner has field-ready documentation and seller toolkits including a clear product value proposition that can be articulated to the AWS sales organization with all relevant information needed to determine fit for a customer opportunity (e.g., sales collateral, presentation, and customer use cases). Evidence must be in the form of sales collateral including a presentation, one-pager, and use-case checklist. Pricing and/or information regarding terms between the APN Partner and the end customer should be removed from this presentation.	
4.2 Product Support/Help Desk	APN Partner offers product support via web chat, phone, or email support to customers.	

	Evidence must be in the form of description of support offered to customers for their product or solution.	
4.3 Product is listed on AWS Marketplace	APN Partner makes solution available via AWS Marketplace. ☐ Yes ☐ No If "yes", APN Partner must provide a link to the AWS Marketplace listing. If "no", no further information is required. Note, AWS Marketplace is not mandatory to achieve the competency	
5.0 APN Partner Self-Assessment		**Met Y/N**
5.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance to the requirements of the AWS Security Technology Partner Validation Checklist. ▪ APN Partner must complete all sections of the checklist. ▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com**, using the following convention for the email subject line: "[APN Partner Name], Security Competency Technology Partner Completed Self-Assessment." ▪ It is recommended that APN Partner has their AWS Partner Solutions Architect, PDR, or PDM review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the APN Partner's AWS team is engaged and working to provide recommendations prior to the review and to help ensure a productive review experience.	

Security Competency Technology Partner Validation Checklist

The following items will be validated by the third-party auditors and/or AWS Partner Solutions Architects; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

General Technical Requirements		Met Y/N
Requirements applicable to all AWS Competency categories		
All solutions must be deployable in at least ten (10) AWS regions		
Solution must have no critical findings across all pillars of an AWS Well-Architected Review		
Solutions that rely on assuming x-account roles for high volume API calls must be architected to include all or a major subset of the following guidelines to reduce AWS API calls: • *The ability to continuously ingest AWS CloudTrail to detect new resources created* • *Incremental back off on API calls* • *The ability to mitigate AWS APIs call activity via API caching* • *The ability to mitigate constant polling of AWS APIs by using Amazon CloudWatch Events and push events*		
All systems must be multi-AZ and demonstrate how they remain highly available and recover in the event of AZ failure		
Must have the option of granular/consumption-based billing/licensing		
Solutions must support centralized management across accounts/regions/VPCs		
Solutions must support centralized logging that can function without direct network connectivity (e.g. use Amazon Simple Notification Service (Amazon SNS)/Amazon Simple Storage Service (Amazon S3))		
For a complex, multi-part solutions (e.g. auto-scaling) there must be an AWS CloudFormation template and accompanying document on how to easily deploy the solution.		

Thorough documentation and deployment guide which could include very detailed step-by-step documentation for AWS setup and deployment This should include videos, blog posts, reference architectures, and sample policies.		

Security Category Specific Technical Requirements		Met Y/N
Required Solution Features Documentation describing how the APN Partner solution meets the requirements must be submitted as part of the competency self-assessment		
Network and Infrastructure Security	*Primary design requirement is how inline devices support a highly available architecture. This Includes: Integration with Autoscaling, Integration with AWS Elastic Load Balancing, Ability to run in a multi Availability Zone (AZ) configuration, Ability to support bootstrapping for automated configuration, Worker/support nodes must use AWS Lambda/Step Functions instead of long-lived Amazon EC2 instances*	
	Networking appliances must support most support modern instances C5/M5/etc. with driver support for ENA/NVMe (AWS Nitro Platform)	
	IDS/IPS must support enrichment of rulesets/detections via ingestion of Amazon GuardDuty Findings	
Host and Endpoint Security	*Support for ingestion of Amazon EC2/VPC Metadata*	
	Support for ingestion and displaying/filtering of Tags (when/if role is available)	
	Ability to identify all instances that are lacking a working agent	
	Ability to protect containers and integrate with one (1) of the following: Amazon ECS, Amazon EKS, and AWS Fargate	
	A logging mechanism must exist which includes Amazon EC2 Metadata (instance ID, account, VPC-id, etc.)	
	Support for Amazon Linux	
Data Protection and Encryption	*Must support AWS Key Management Service (KMS) as source of truth to support use KMS vended keys* *Or* *Ability to integrate with AWS CloudHSM for the above requirements*	
	DLP must evaluate Amazon S3 bucket policies for open/public buckets	
	Solutions must support ingestion of Amazon S3 object level API activity in AWS CloudTrail	
	DLP must support Amazon S3 objects and evaluate Amazon S3 policies as part of solution	
	DLP must integrate with alerts from Amazon Macie	
Governance, Risk, and Compliance	*Solution must explicitly state what frameworks and controls solution fulfill and/or evaluate* *Examples Include: PCI-DSS, HIPAA, FIPS 140-2, NIST 800-53, GDPR, SOC2, and CIS*	
	Ability to evaluate against CIS Benchmarks for AWS	
	CMDBs must have the ability to ingest data from AWS Config and/or AWS CloudTrail	
	Ability to detect changes in environment with AWS CloudTrail	

	Ability to leverage CloudTrail, Config/Config Rules/CloudFormation to maintain desired state guardrails	
	Ability to Evaluate Changes in AWS Policies and posture in a maximum of 1 hour	
	Integration with AWS Security Hub	
Logging, Monitoring, Threat Detection, and Analytics	*Must be able to consume 4+ of the following: AWS CloudTrail, VPC Flowlogs, Amazon Route 53 Query Logs, AWS WAF Logs, AWS X-Ray Logs, Amazon RDS Logs, AWS Config Data, Amazon Inspector Findings, Amazon GuardDuty, Amazon Macie Alerts, and Amazon EBS Logs*	
	Support and describe ability for high velocity ingestion of logs via Kinesis, CWE, SQS, Lambda and must minimize features like the CloudTrail LookupEvents API.	
	Integration with AWS Security Hub	
Identity and Access Control	*Provide multi-account federated SSO access to the AWS Management Console*	
	Provide a mechanism for federated AuthN/AuthZ to AWS APIs via the command line	
	Privileged User Manager must provide Auditing and Evaluation of IAM Policy Documents	
	Provide SAML Authentication to AWS Services such as Amazon Redshift, Amazon Cognito, AWS Appstream, Amazon Connect, and Amazon Quicksight	
	Provide Multi-Factor Authentication as an option	
Vulnerability and Configuration Assessment	*Vulnerability Scanner must use AWS 'describe' API calls to enumerate scan target IP addresses*	
	Must provide centralized mechanisms to scan in a multi-account/region/vpc environment	
	Must provide remediation guidance when there are findings	
	Must have the ability to assess the following policy types: S3 Bucket Policies, IAM Policies	
	Ability to assess customer AWS account and service configuration against recommended best practices, such as: Well-Architected Security Pillar Whitepaper and CIS AWS Benchmarks.	
	Integration with AWS CloudTrail in order to be able to identify mutating events or new resources in the customer's account.	
Application Security	*WAFs must support modern instance (C5/M5) and AWS Nitro System*	
	RASP/Code Analysis Tools must integrate with AWS CodeStar Services	

		Applies to:		
Technical Validation		SaaS	Customer-Deployed on AWS	Met Y/N
Architecture Diagram	Depending on the Deployment Category, one or more Architecture Diagrams are required. Each Architecture Diagram must show: ☐ The major elements of the architecture, and how they combine to provide the APN Partner Solution to customers ☐ All of the AWS services used, using the appropriate AWS service icons. ☐ How the AWS services are deployed, including, VPCs, AZs, subnets, and connections to systems outside of AWS.	Yes – one for the whole solution and one for each Case Study.	Yes – one for each Case Study.	

	☐ Includes elements deployed outside of AWS, e.g. on-premises components, or hardware devices.			
Deployment Guide	The Deployment Guide must provide best practices for deploying the APN Partner Solution on AWS, and include all of the sections outlined in "Baseline Requirements for Deployment Guides"	No	Yes – one for the solution.	
Completed Validation Checklist	For each of the four (4) Case Studies provided for the APN Partner Solution, the APN Partner must provide a completed version of the following checklist indicating which checklist items are met per case study.	Yes	Yes	
1.0 Security **The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.**				
1.1 AWS account root user is not used for routine activities	The AWS account root user must not be used for routine activities. Following the creation of your AWS account, you should immediately create IAM user accounts, and use these IAM user accounts for all routine activities. Once your IAM users accounts have been created, you should securely store the AWS root account credentials and use them only to perform the few account and service management tasks that require the AWS account root user. For further information on how to set up an IAM user accounts and groups for daily use, see Creating Your First IAM Admin User and Group.	Yes	No	
1.2 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user	MFA must be enabled for your AWS account root user. Because your AWS account root user can perform sensitive operations in your AWS account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available, including virtual MFA and hardware MFA.	Yes	No	
1.3 IAM user accounts used for all routine activities	The AWS account root user must not be used for any task where it is not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an Administrators group to which you attach the AdministratorAccess managed policy. Thereafter, the users in the administrator's group should set up the groups, users, and so on, for the AWS account. All future interaction should be through the AWS account's users and their own keys instead of the root user. However, to perform some account and service management tasks, you must log in using the root user credentials.	Yes	No	
1.4 Multi-Factor Authentication (MFA) is enabled for all interactive IAM users	You must enable MFA for all interactive IAM users. With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).	Yes	No	
1.5 IAM credentials are rotated regularly	You must change your passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords, and you can choose how often they must do so. For more information about rotating access keys for IAM users, see Rotating Access Keys.	Yes	Yes (for credentials used to integrate with AWS)	
1.7 Strong password policy	You must configure a strong password policy for your IAM users. If you allow users to change their own passwords, require that	Yes	Yes (for credentials	

is in place for IAM users	they create strong passwords and that they rotate their passwords periodically. On the Account Settings page of the IAM console, you can create a password policy for your account. You can use the password policy to define password requirements, such as minimum length, whether it requires non-alphabetic characters, how frequently it must be rotated, and so on. For more information, see Setting an Account Password Policy for IAM Users.		used to integrate with AWS)	
1.8 IAM credentials are not shared among multiple users	You must create an individual IAM user account for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative privileges, and use that IAM user for all your work. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)	Yes	No	
1.9 IAM policies are scoped down to least privilege	You must follow the standard security advice of granting least privilege. This means granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.	Yes	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	
1.10 Hard-coded credentials (e.g. access keys) are not used	You must follow best practices for managing AWS access keys and avoid the use of hard-coded credentials. When you access AWS programmatically, you use an access key to verify your identity and the identity of your applications. Anyone who has your access key has the same level of access to your AWS resources that you do. Consequently, AWS goes to significant lengths to protect your access keys, and, in keeping with our shared responsibility model, you should as well.	Yes	Yes (credentials used to integration with AWS should be easily changed and not hard coded)	
1.11 All credentials are encrypted at rest	The baseline requirement is to ensure the encryption of any credentials at rest.	Yes	Yes	
1.12 AWS Access Keys only used by interactive users	No AWS Access Keys should be in use, except in the following cases: 1. Used by humans to access AWS services, and stored securely on a device controlled by that human. 2. Used by a service to access AWS services, but only in cases where: a) It is not feasible to use an EC2 instance role, ECS Task Role or similar mechanism, b) The AWS Access Keys are rotated at least weekly, and c) The IAM Policy is tightly scoped so that it: i) Allows only access to only specific methods and targets and ii) Restricts access to the subnets on from which the resources will be accessed.	Yes	No	
1.13 CloudTrail is enabled for all AWS accounts in every region	AWS CloudTrail must be enabled on all AWS accounts and in every region. Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when	Yes	No	

	the event occurred, and other details to help you analyze and respond to activity in your AWS account.			
1.14 CloudTrail logs are stored in an S3 bucket owned by another AWS account	CloudTrail logs must be emplaced in a bucket owned by another AWS account configured for extremely limited access, such as audit and recovery only.	Yes	No	
1.15 CloudTrail S3 log bucket has Versioning or MFA Delete enabled	CloudTrail log bucket contents must be protected with versioning or MFA Delete.	Yes	No	
1.16 EC2 security groups are tightly scoped	All EC2 security groups should restrict access to the greatest degree possible. This includes at least 1. Implementing Security Groups to restrict traffic between Internet and VPC, 2. Implementing Security Groups to restrict traffic within the VPC, and 3. In all cases, allow only the most restrictive possible settings.	Yes	Yes	
1.17 S3 buckets within your account have appropriate levels of access	You must ensure that the appropriate controls are in place to control access to each S3 bucket. When using AWS, it's best practice to restrict access to your resources to the people that absolutely need it (the principle of least privilege).	Yes	No (unless APN Partner solution running on AWS requires the S3 service)	
1.18 S3 buckets have not been misconfigured to allow public access.	You must ensure that buckets that should not allow public access are properly configured to prevent public access. By default, all S3 buckets are private, and can only be accessed by users that have been explicitly granted access. Most use cases won't require broad-ranging public access to read files from your S3 buckets, unless you're using S3 to host public assets (for example, to host images for use on a public website), and it's best practice to never open access to the public.	Yes	No (unless APN Partner solution running on AWS requires the S3 service)	
1.19 A monitoring mechanism is in place to detect when S3 buckets or objects become public	You must have monitoring or alerting in place to identify when S3 buckets become public. One option for this is to use Trusted Advisor. Trusted Advisor checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. The Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.	Yes	No (unless APN Partner solution running on AWS requires the S3 service)	
1.20 A monitoring mechanism is in place to detect changes in EC2 instances and Containers	Any changes to your EC2 instances or Containers may indicate unauthorized activity, and must at a minimum be logged to a durable location to allow for future forensic investigation. The mechanism employed for this purpose must at least: 1. Detect any changes to the OS or application files in the EC2 instances or Containers used in the solution. 2 Store data recording these changes in a durable location, external to the EC2 instance or Container. Examples of suitable mechanisms include: a. Deployment of file integrity checking via scheduled configuration management (e.g. Chef, Puppet, etc.) or a specialized tool (e.g. OSSEC, Tripwire or similar), or b. Extending configuration management tooling to validate EC2 host configuration, and alert	Yes	No	

	on updates to key configuration files or packages with 'canary' (logged no-op) events configured to ensure the service remains operational on all in-scope hosts during runtime, or c. Deploying a Host Intrusion Detection System such as an open source solution like OSSEC with ElasticSearch and Kibana or using a APN Partner solution. Note that the following mechanism does not meet this requirement: a. Frequently cycling EC2 instances or Containers.			
1.21 All data is classified	All customer data processed and stored in the workload is considered and classified to determine its sensitivity and the appropriate methods to use when handling it.	Yes	No	
1.22 All sensitive data is encrypted	All customer data classified as sensitive is encrypted in transit and at rest.	Yes	No	
1.23 Cryptographic keys are managed securely	All cryptographic keys are encrypted at rest and in transit, and access to use the keys is controlled using an AWS solution such as KMS or an APN Partner solution such as HashiCorp Vault.	Yes	Yes	
1.24 All data in transit is encrypted	All data in transit across a VPC boundary is encrypted.	Yes	Yes	
1.25 Security incident response process is defined and rehearsed	A security incident response process must be defined for handling incidents such as AWS account compromises. This process must be tested by implementing procedures to rehearse the incident response process, e.g. by completing a security game day exercise. A rehearsal must have been held within the last 12 months to confirm that: a. The appropriate people have access to the environment. b. The appropriate tools are available. c. The appropriate people know what to do to respond to the various security incidents outlined in the plan.	Yes	No	
2.0 Reliability The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.				
2.1 Network connectivity is highly available	Network connectivity to the solution must be highly available. If using VPN or Direct Connect to connect to customer networks, the solution must support redundant connections, even if the customers do not always implement this.	Yes	Yes	
2.2 Infrastructure scaling mechanisms align with business requirements	Infrastructure scaling mechanisms must align with business requirements, either by: 1. Implementing auto-scaling mechanisms at each layer of the architecture, by 2. Confirming that current business requirements, including cost requirements and anticipated user growth, do not require auto-scaling mechanisms AND manual scaling procedures are fully documented and frequently tested.	Yes	Yes	
2.3 AWS and Application logs are managed centrally	All log information from the application, and from the AWS infrastructure, should be consolidated into a single system.	Yes	No	
2.4 AWS and Application monitoring and alarms are managed centrally	The application and the AWS infrastructure must be monitored centrally, with alarms generated and sent to the appropriate operations staff.	Yes	No	
2.5 Infrastructure provisioning and	The solution must use an automated tool such as CloudFormation or Terraform to provision and manage the AWS infrastructure. The AWS Management Console must not be used to make	Yes	No	

management is automated	routine changes to the production AWS infrastructure.			
2.6 Regular data backups are being performed	You must perform regular backups to a durable storage service. Backups ensure that you have the ability to recover from administrative, logical, or physical error scenarios. Amazon S3 and Amazon Glacier are ideal services for backup and archival. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. The pay-for-what- you-use model and low cost per GB/month make these services a good fit for data protection use cases.	Yes	No	
2.7 Recovery mechanisms are being tested on a regular schedule and after significant architectural changes	You must test recovery mechanisms and procedures, both on a periodic basis and after making significant changes to your cloud environment. AWS provides substantial resources to help you manage backup and restore of your data.	Yes	No	
2.8 Solution is resilient to availability zone disruption	The solution must continue to operate in the case where all of the services within a single availability zone have been disrupted.	Yes	Yes	
2.9 Resiliency of the solution has been tested	The resiliency of the infrastructure to disruption of a single availability zone has been tested in production, e.g. through a game day exercise, within the last 12 months.	Yes	Yes	
2.10 Disaster Recovery (DR) plan has been defined	A well-defined Disaster Recovery plan includes a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO). You must define an RPO and an RTO for all in-scope services, and the RPO and RTO must align with the SLA you offer to your customers	Yes	No	
2.11 RTO is less than 24 hours	The baseline requirement is for the RTO to be less than 24 hours for core services.	Yes	No	
2.12 Disaster Recovery (DR) plan is adequately tested	Your DR plan must be tested against your RPO and RTO, both periodically and after major updates. At least one DR test must be completed prior to approval of your AWS APN Advanced Tier application.	Yes	No	
2.13 DR plan includes recovery to another AWS account	Your DR plan must include a strategy for recovering to another AWS account, and your periodic recovery testing must test this scenario. You must have completed at least one full test of the DR plan, including at least recovery to another AWS account, within the last 12 months. Note: Although processes restoring data into test environments or exporting data for users are useful ways to verify backups, these processes do not fulfill the requirement to perform a full restore test to another AWS account.	Yes	No	
3.0 Operational Excellence The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.				
3.1 Deployment of code changes is automated	The solution must use an automated method of deploying code to the AWS infrastructure. Interactive SSH or RDP sessions must not be used to deploy updates in the AWS infrastructure.	Yes	No	
3.2 Runbooks and escalation process are defined	Runbooks must be developed to define the standard procedures used in response to different application and AWS events. An escalation process must be defined to deal with alerts and alarms generated by the system, and to respond to customer-reported	Yes	No	

	incidents. The escalation process must also include escalating to AWS Support where appropriate.			
3.3 AWS Business Support is enabled for the AWS Account	Business Support must be enabled. Business Support (or greater) is an AWS Partner Network requirement for Advanced Tier Technology APN Partners. To qualify for Advanced Tier, you must enable Business Support on at least one of your AWS accounts.	Yes	No	

AWS Resources

Title	Description
How to Build a Practice Landing Page	Provides guidance how to build a Practice/solution page that will meet the prerequisites of the Program.
How to write a Public Case Study	Provides guidance how to build a Public Customer Case Study that will meet the prerequisites of the Program.
How to build an Architecture Diagram	Provides guidance how to build an architecture diagrams that will meet the prerequisites of the Program.
APN Partner Readiness Doc	Provides guidance and best practice examples of the Program perquisites.
Well Architected Website	Learn about the Well Architected Framework and it's approach.

AWS reserves the right to make changes to the AWS Competency Program at any time and has sole discretion over whether APN Partners qualify for the Program.